A COHOMOLOGICAL TREATISE OF HKG-COVERS WITH APPLICATIONS TO THE NOTTINGHAM GROUP

ARISTIDES KONTOGEORGIS AND IOANNIS TSOUKNIDAS

Abstract. We characterize Harbater-Katz-Gabber curves in terms of a family of cohomology classes satisfying a compatibility condition. Our construction is applied to the description of finite subgroups of the Nottingham Group.

1. Introduction

In this article we use and extend results from previous work of the first author together with S. Karanikolopoulos [14] on HKG-curves. We will work over an algebraically closed field k of characteristic $p \geq 5$.

Definition 1. *A Harbater-Katz-Gabber cover (HKG-cover for short) is a Galois cover $X_{\mathrm{HKG}} \to \mathbb{P}^1$, such that there are at most two branched k-rational points $P_1, P_2 \in \mathbb{P}^1$, where P_1 is tamely ramified and P_2 is totally and wildly ramified. All other geometric points of $\mathbb{P}^1$ remain unramified. In this article we are mainly interested in p-groups so our HKG-covers have a unique ramified point, which is totally and wildly ramified.*

Work of Harbater [9] and of Katz and Gabber [15] showed that any finite subgroup G of $\mathrm{Aut}(k[[t]])$ can be associated with an HKG-curve X. More precisely, G is the semi-direct product of a cyclic group of order prime to p (the maximal tamely ramified quotient) by a normal p-subgroup (the wild inertia group). We are interested in the latter group so from now on we will replace the initial group G with the latter, finite p-subgroup of $\mathrm{Aut}(k[[t]])$. The HKG-curves play an important role in the deformation theory of curves with automorphisms and to the celebrated proof of Oort conjecture, [20, 21, 6, 4, 5, 22].

Working with the HKG-curve X allows us to use several global tools like the genus, the p-rank of the Jacobian etc to the study of $k[[t]]$. In this article we will employ the Weierstrass semigroup attached to the unique ramified point P, and we will use the results of [14] on relating the structure of the Weierstrass semigroup to the jumps of the ramification filtration.

More precisely to the HKG-cover there is a Weierstrass semigroup $H(P)$ attached to the unique wildly ramified point P. An arithmetic semigroup, and in particular the Weierstrass semigroup, is always finitely generated i.e. there are $\bar{m}_1, \ldots, \bar{m}_h \in \mathbb{N}$ such that
$$H(P) = \mathbb{Z}_+ \bar{m}_1 + \cdots + \mathbb{Z}_+ \bar{m}_h.$$
We will denote by m_i the i-th element of $H(P)$, while $\bar{m}_i$ will denote the i-th generator of the semigroup. For every element $m_i \in H(P)$ we will select a function f_i with $(f_i)_\infty = m_i P$. Also each element $\bar{m}_i$ corresponds to some function $\bar{f}_i$ in the function field of the curve. This selection is not unique and we will study later what happens by different choices either of f_i or $\bar{f}_i$. The ramification filtration gives rise to a series of subgroups of the group G, see eq. (3), which corresponds to a sequence of subfields $k(X/G) = F_0 \subset \cdots \subset F_{s+1} = k(X)$ of the function field $F = k(x)$ of the curve X. By the properties of the ramification filtration, each extension F_{i+1}/F_i, $i = 0, \ldots, s$ is abelian. We will see that $F_{i+1} = F_i(\bar{f}_i)$.

One of the main results of this article is the classification and description of the Galois actions in HKG-covers in terms of group cohomology. Assume that $X \to \mathbb{P}^1$ is an HKG-cover with a unique wildly ramified point $P \in X$. Consider the ring of holomorphic functions outside the point P

$$\mathbf{A} = \bigcup_{\nu=0}^{\infty} L(\nu P).$$

This ring is equipped with a valuation and elements of $\mathbf{A}$ of valuation smaller than ν, i.e. the Riemann-Roch space $L(\nu P)$, give rise to a finite vector space. Notice that these kind of rings are essential in the general definition of Drinfeld modules, see [8, chap. 4].

The elements of degree smaller that n can be represented as polynomials of bounded degree as follows; for every $\mathbf{n} = (n_1, \ldots, n_s) \in \mathbb{N}^s$ and $m \in \mathbb{N}$ we will define in eq. (10) the vector space $k_{\mathbf{n},m}[\bar{f}_0, \ldots, \bar{f}_s]$ which will be considered as a G-module and prove that it is equal to $L\big((m-1)P\big)$.

The action of G will be described by the following:

Theorem 2. *The G-module structure of $k_{\mathbf{n},m}[\bar{f}_0, \ldots, \bar{f}_s]$ is described by a series of cohomology classes $\bar{c}_i \in H^1(\mathrm{Gal}(F_{i+1}/F_1), k_{\mathbf{n},m_{i+1}}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$. These classes restricted to the elementary abelian group $\mathrm{Gal}(F_{i+1}/F_i)$ define the additive polynomials $P_i(Y)$ which in turn describe the elementary abelian extensions F_{i+1}/F_i. These polynomials P_i define maps*

$$H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]) \longrightarrow H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$$

and the cocycles $\bar{c}_i$ are in the kernel of P_i, that is

(1) $$P(\bar{c}_i) = 0 \in H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]).$$

Conversely every such series of elements $\bar{c}_i \in H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$, satisfying eq. (1) defines in a unique way a HKG-cover.

Proof. That the change of basis gives rise to coboundaries will be discussed in lemma 11. The definition of the additive polynomials P_i and the compatibility condition is given in theorems 13 and 15.

We will now see how we can construct the HKG-cover from the information of the compatible classes $\bar{c}_i \in H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$. We said that the additive polynomials can be constructed from the classes $\bar{c}_i$. The compatibility equation $P_i(\bar{c}_i) = 0$ gives us that the cocycle representative $\bar{c}_i$ is a coboundary, that is there is an element $b_i \in k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$ such that $P_i\big(\bar{c}_i(\sigma)\big) = (\sigma - 1)b_i$ for all $\sigma \in G$. But then the element $\bar{f}_i$ satisfies the generalized Artin-Schreier extension

(2) $$P_i(\bar{f}_i) = b_i,$$

see section 2.6. This essentially means that we can construct the HKG-cover step by step, adding in each step the generator $\bar{f}_i$ satisfying eq. (2). $\qquad\square$

In fact the above theorem states that all the information for the HKG-cover is inside the sequence of compatible cohomology classes. This result is similar to the cohomological interpretation of Kummer and Artin-Schreier-Witt extensions, see [11, 8.9-8.11], [19, chap. VI, sec. 1-2]. Of course Kummer and Artin-Schreier-Witt extensions are abelian, while the HKG-extensions are solvable. This fits well with the Shafarevich philosophy as expressed in [24].

As an application of the above result we give the following description of finite automorphism p-groups of the Nottingham group:

Theorem 3. *Let G be a finite p-subgroup of the Nottingham group. There are elements $\bar{f}_0, \ldots, \bar{f}_s \in k[[t]]$ acted on by G in terms of the cohomology classes $\bar{c}_i$ as described in theorem 2, and a local uniformizer $t' = \bar{f}_s^{1/m}$ so that*

$$\sigma(t') = t'(1 + \bar{c}_s(\sigma)t'^m)^{-1/m} \in k[[t']] = k[[t]], \text{ for every } \sigma \in G.$$

Proof. See theorem 16 and the discussion following it.   □

The above theorem is applied as follows: We start from a local action of a finite p-group on $\mathrm{Aut}(k[[t]])$ and we construct an HKG-cover from it. From this HKG-cover we obtain the series of generators $\bar{f}_0, \ldots, \bar{f}_s \in k[[t]][t^{-1}]$ and we define the cohomology class $\bar{c}_s$, which in turn gives an explicit form of the action of G on $k[[t']]$. Essentially we describe the conjugation class of $G \subset \mathrm{Aut}(k[[t]])$, since the group acting on $k[[t]]$ by

$$\sigma(t) = t(1 + \bar{c}_s(\sigma)t^m)^{-1/m},$$

is conjugate to our original action.

We now describe the structure of this article. In section 2 we will introduce the representation and ramification filtration and their relation and we will also give a description of the Riemann-Roch space $L(m_iP)$ as polynomials of bounded degrees. In section 2.5.1 we will interpret flags of Riemann-Roch spaces as a categorification of the set of arithmetic semigroups. Then we give a cohomological interpretation of the action of the group G and we also see how the polynomials of each successive abelian extension can be recovered from this construction. In section 3 we apply these tools in the problem of determining finite subgroups of the Nottingham group and in particular we give explicit forms of elements of order p^h. In the cyclic group case the cohomology group can be expressed in terms of coinvariants of group action, see proposition 22. It seems that in recent years interest on this problem has grown, see [16], [1], [18], [26].

2. Generalities on HKG-covers

2.1. **Ramification filtration.** In the associated HKG-curve, the group G will coincide with the inertia group of the curve at the unique ramified point, $G_T(P) = \{\sigma \in G(P) : v_p(\sigma(t) - t) \geq 1\}$, where t is a local uniformizer at P and v_P is the corresponding valuation. For more information on ramification filtration the reader is referred to [23]. We define $G_i(P)$ to be the subgroup of $\sigma \in G(P)$ that acts trivially on $\mathscr{O}_p/m_P^{i+1}$, obtaining the following filtration;

(3) $$G_T(P) = G_0(P) = G_1(P) \supseteq G_2(P) \supseteq \cdots \supseteq \{1\}.$$

Let us call an integer i a *jump of the ramification filtration* if $G_i(P) \gneqq G_{i+1}(P)$ and denote by
(4)
$$G_0(P) = G_1(P) = \cdots = G_{b_1}(P) \gneqq G_{b_1+1}(P) = \cdots = G_{b_2}(P) \gneqq \cdots \gneqq G_{b_\mu}(P) \gneqq \{1\}$$

the filtration of the jumps, assuming that there are μ jumps.

2.2. **The Weierstrass semigroup.** The Weierstrass semigroup $H(P)$ is the semigroup consisted of all pole numbers, i.e. $m \in \mathbb{N}$, such that there is a function f on X with $(f)_\infty = mP$. For the Weierstrass semigroup $H(P)$ we consider all pole numbers m_i forming an increasing sequence

$$0 = m_0 < \ldots < m_{r-1} < m_r,$$

where m_r is the first pole number not divisible by the characteristic. If $g \geq 2$ and $p \geq 5$ we can prove that $m_r \leq 2g - 1$, see [17].

Let $F = k(X)$ be the function field of the HKG-curve X. For every m_i, $0 \leq i \leq r$ in the Weierstrass semigroup we denote by $f_i \in F$ an element of F that has a unique pole at P of order m_i, i.e. $(f_i)_\infty = m_i P$. For each $i \in \{0, \ldots, r\}$ the set $\{f_0, \ldots, f_i\}$ forms a basis for the Riemann-Roch space $L(m_i P)$. The spaces

(5) $$k = L(m_0 P) \subsetneq L(m_1 P) \subsetneq \cdots \subsetneq L(m_r P)$$

give rise to a natural flag of vector spaces corresponding to the Weierstrass semi-group. Notice that if μ is a pole number in $H(P)$ we have $\mu = m_{\dim L(\mu P) - 1}$.

2.3. **Representation filtration.** For each $0 \leq i \leq r$ we consider the representations

(6) $$\rho_i : G_1(P) \to \mathrm{GL}(L(m_i P))$$

which give rise to a decreasing sequence of groups

(7) $$G_1(P) = \ker\rho_0 \supseteq \ker\rho_1 \supseteq \ker\rho_2 \supseteq \ldots \supseteq \ker\rho_r = \{1\}.$$

Recall that r is the index of m_r, the first pole number not divisible by p. In [17] the first author proved that ρ_r is faithful and the last equality $\ker\rho_r = \{1\}$ follows.

We shall call the last filtration the *representation filtration of G*.

Definition 4. *An index i is called a jump of the representation filtration if and only if $\ker\rho_i \gneqq \ker\rho_{i+1}$.*

We will denote the jumps in the representation filtration by

$$c_1 < c_2 < \ldots < c_{n-1} < c_n = r - 1,$$

that is

$$\ker\rho_{c_i} > \ker\rho_{c_i+1}.$$

The last equality $c_n = r - 1$ is proved in [13, rem. 9]. We have now a sequence of decreasing groups

(8) $$G_1(P) = \ker\rho_0 = \ldots = \ker\rho_{c_1} > \ldots \ker\rho_{c_{n-1}} > \ker\rho_{c_n} > \{1\}$$

which gives rise to the following sequence of extensions;

(9) $$F^{G_1(P)} = F^{\mathrm{Ker}\rho_{c_1}} \subset F^{\mathrm{Ker}\rho_{c_2}} \subset \cdots \subset F^{\mathrm{Ker}\rho_{c_n}} \subset F.$$

2.4. **A relation of the two filtrations in the case of HKG-covers.** In [14] Karanikolopoulos and the first author related the filtrations defined in eq. (4), (8) and the Weierstrass semigroup in the following way;

Theorem 5. *We distinguish the following two cases:*
• *If $G_1(P) > G_2(P)$ then the Weierstrass semigroup is minimally generated by $m_{c_i+1} = p^{h_i}\lambda_i$, $(\lambda_i, p) = 1$, $1 \leq i \leq n$ and the cover $F/F^{G_2(P)}$ is an HKG-cover as well. In this case $|G_2(P)| = m_1$.*
• *If $G_1(P) = G_2(P)$ then the Weierstrass semigroup is minimally generated by $m_{c_i+1} = p^{h_i}\lambda_i$, $(\lambda, p) = 1$, $1 \leq i \leq n$ and by an extra generator $p^h = |G_1(P)|$, which is different by all m_{c_i+1} for all $1 \leq i \leq n$.*

Especially when $X \to \mathbb{P}^1$ is an HKG-cover, the number of ramification jumps μ coincides with the number of representation jumps n, i.e. $n = \mu$. The integers λ_i, which appear as factors of the integers m_{c_i+1}, $1 \leq i \leq n$ are the jumps of the ramification filtration, i.e. $\lambda_i = b_i$ and $G_{b_i} = \mathrm{Ker}\rho_{c_i}$ for $2 \leq i \leq n$. Summing up we have the following options for the ramification filtration

$$G_1(P) = \cdots = G_{\lambda_1} \gneqq G_{\lambda_1+1} = \cdots = G_{\lambda_2} \gneqq G_{\lambda_2+1} = \cdots = G_{\lambda_n} \gneqq \{1\}$$

or

$$G_1(P) > G_2(P) = \cdots = G_{\lambda_1} \gneqq G_{\lambda_1+1} = \cdots = G_{\lambda_2} \gneqq G_{\lambda_2+1} = \cdots = G_{\lambda_n} \gneqq \{1\}$$

Proof. See [14, th. 13,th. 14]. □

Remark 6. *The reader should notice that* $\mathrm{Ker}\rho_{c_1} = \mathrm{Ker}\rho_0 = G_1(P) = G_{b_1}(P)$ *by definition, hence* $G_{b_i} = \mathrm{Ker}\rho_{c_i}$ *for every* $i \in \{1, \ldots, n = \mu\}$.

Theorem 5 allows us to use the well known fact that the quotients $G_{b_i}/G_{b_{i+1}}$ are elementary abelian p-groups, hence the quotients $\mathrm{Ker}\rho_{c_i}/\mathrm{Ker}\rho_{c_{i+1}}$ are elementary abelian too, and the corresponding sequence of fields in (9) is in fact, a sequence of elementary abelian p-group extensions.

In [14, prop. 27] the first author and S. Karanikolopoulos observed that for a $\sigma \in \mathrm{Ker}\rho_{c_i} - \mathrm{Ker}\rho_{c_{i+1}}$ the following hold;

$$\sigma(f_\nu) = f_\nu \text{ for all } \nu \le c_i$$

$$\sigma(f_{c_i+1}) = f_{c_i+1} + c(\sigma) \text{ for some } c(\sigma) \in k^*.$$

They also proved (prop. 20 & rem. 21) that for each $i \in \{1, \ldots, n\}$ we have $F^{\ker \rho_{c_{i+1}}} = F^{\ker \rho_{c_i}}(f_{c_i+1})$.

In order to simplify notation we set $F_i := F^{\ker \rho_{c_i}}$, $\bar{m}_i := m_{c_i+1}$ and $\bar{f}_i := f_{c_i+1}$, see also eq. (10).

Example 7. *The Artin-Schreier extension* $F = k(x)(y)$ *where* $y^p - y = x^m$, *has ramification filtration,* [25, prop. 3.7.8]

$$\mathbb{Z}/p\mathbb{Z} = G_0 = \cdots = G_m > \{1\},$$

i.e. the first and unique ramification jump is at m. The representation filtration is given by

$$G_0 = \ker\rho_0 = \cdots = \ker\rho_{m-1} > \{1\},$$

that is, the first representation jump is at $c_1 = m - 1$ and $\bar{f}_1 = f_{c_1+1} = y$, where $c_1 = m - 1$ and $c_1 + 1 = m$. Thus $F = F_2 = F_1(\bar{f}_1)$, and $\bar{f}_0$ is the generator x of the rational function field $k(x)$.

We will prove in section 2.6 the following

Proposition 8. *For a given $m \in H(P)$, in the case of HKG-covers we have*

$$L\big((m-1)P\big) = k_{\mathbf{n},m}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_s],$$

where

$$(10) \quad k_{\mathbf{n},m}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_s] = \left\langle \begin{array}{c} \bar{f}_0^{a_0} \bar{f}_1^{a_1} \cdots \bar{f}_s^{a_s} : 0 \le a_i < p^{n_i} \text{ for all } 1 \le i \le s, \\ \text{and } \deg(\bar{f}_0^{a_0} \bar{f}_1^{a_1} \cdots \bar{f}_s^{a_s}) = \sum_{\nu=0}^{s} a_\nu \bar{m}_\nu < m \end{array} \right\rangle_k.$$

The integer s is determined uniquely; it is the greatest index of $\bar{m}_i$ such that $\bar{m}_i < m$ holds. The quantity $\mathbf{n} = (n_1, \ldots, n_s) \in \mathbb{N}^s$ depends on the ramification filtration, specifically n_i is the number of $\mathbb{Z}/p\mathbb{Z}$ components in each elementary abelian group G_i/G_{i+1} obtained by quotients of the lower ramification filtration.

2.5. Categorification of the Weierstrass semigroup.

2.5.1. *Categorification.* The Weierstrass semigroup $H(P)$ can be embedded into the semigroup $\mathrm{Div}^+(X)$ of effective divisors, by sending

$$H(P) \ni n \mapsto nP \in \mathrm{Div}^+(X).$$

Moreover to the semigroup $H(P)$ we can attach a flag of vector spaces $L(nP)$.

Recall that the categorification is the process of replacing set-theoretic notions by category-theoretic equivalents. In decatecorification process, which is the inverse process of categorification, isomorphic objects in a category become equal.

We will define now a category $\mathscr{F}$ in order to categorify the set of numerical semigroups. The objects of $\mathscr{F}$ are families of invertible sheaves $(\mathscr{L}_i)_{i=1}^{\infty}$, corresponding to divisors D_i (see [10, prop. 6.13, p. 144]) so that $0 \le D_i < D_j$ for $i < j$ and $\mathscr{L}_i \otimes \mathscr{L}_j$ is an element of the family, i.e. $\mathscr{L}_i \otimes \mathscr{L}_j \cong \mathscr{L}_{n(i,j)}$, for some

$\mathbb{N} \ni n(i, j) \geq i, j$. Observe that isomorphic line bundles give rise to linear equivalent divisors, [10, prop. 6.13c]. The maps in the category $\mathscr{F}$ are families of maps of invertible sheaves. The decategorification map sends isomorphic families of invertible sheaves to the numerical semigroup $\left(\deg(\mathscr{L}_i)\right)_{n=1}^{\infty}$.

To an object of $\mathscr{F}$ we can attach the flag of k-vector spaces

$$k = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_m \subsetneq \cdots$$

where $V_i = H^0(X, \mathscr{L}_i)$. Also we notice that if V_i, V_j are in the flag then $H^0(X, \mathscr{L}_i \otimes \mathscr{L}_j)$ is in the flag.

The functions in the category $\mathscr{F}$ induce families of linear maps $f_i : V_i \to W_i$ such that $f_i \mid_{V_\nu} = f_\nu$ for all $\nu < i$ and all $i \in \mathbb{N}$. In particular $f_i(V_\nu) \subset W_\nu$ for all $\nu < i$, $i \in \mathbb{N}$.

2.5.2. *Groups acting on flags.* An automorphism of a curve act on all "invariants" of the curve including the Weierstrass semigroup of the unique ramified point. Usually this action on invariants provides useful information about the action. Unfortunately the action of the group G on the semigroup $H(P)$ is trivial. This is not the case for the categorification, we will see that the group acts faithfully on the corresponding flag.

We will say that a group G is acting on a flag $\bar{V}$, if there is a homomorphism

$$\rho : G \to \mathrm{Aut}(\bar{V}),$$

i.e. when $\rho(g)$ is an isomorphism in the category of flags.

Remark 9. *Since the representation ρ_r is faithful it makes sense to consider the representation not on the whole flag but only up to $L(m_r P)$. The natural isomorphisms on this truncated flag are given by invertible upper triangular matrices.*

For every $1 \leq i \leq s$ we have that

$$\sigma(f_i) = f_i + c_i(\sigma), \text{ where } c_i(\sigma) \in L\big((m_i - 1)P\big).$$

Proposition 8, which will be proved in the next section, implies that if $\bar{f}_1, \ldots, \bar{f}_s$ are fixed, then the values $\bar{c}_i$ for $1 \leq i \leq s$ determine the action completely. Notice that f_i are polynomial expressions on $\bar{f}_1, \ldots, \bar{f}_s$. By proposition 8 we have $\bar{c}_i \in L\big((\bar{m}_i - 1)P\big) = k_{\mathbf{n}, \bar{m}_i}[\bar{f}_0, \ldots, \bar{f}_{i-1}]$. The functions $\sigma \mapsto c_i(\sigma)$ and $\sigma \mapsto \bar{c}_i(\sigma)$ are cocycles, i.e.

$$\bar{c}_i(\sigma\tau) = \bar{c}_i(\sigma) + \sigma\bar{c}_i(\tau).$$

We plan to show that these cocycles define the action of G on X, and in particular the finite subgroup of $\mathrm{Aut}k[[t]]$.

Remark 10. *The selection of the generators $\bar{f}_i$ for $0 \leq i \leq s$ is not unique. Every element $a \in k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]$ gives rise to a new generator $\bar{f}_i + a$.*

The new cocycle $\bar{c}'_i$ which is defined in terms of the generator $\bar{f}_i + a$ is given by

$$\sigma(\bar{f}_i + a) = \sigma(\bar{f}_i) + \sigma(a) = \bar{f}_i + a + \bar{c}_i(\sigma) + \sigma(a) - a = \bar{f}_i + a + \bar{c}'_i(\sigma).$$

Therefore

$$\bar{c}'_i(\sigma) = \bar{c}_i(\sigma) + (\sigma - 1)a.$$

This gives us the following

Lemma 11. *The cocycles $\bar{c}_i, \bar{c}'_i$ corresponding to different generators $\bar{f}_i, \bar{f}'_i$ with the same pole number $\bar{m}_i$ differ by a coboundary and a generaror free description of the action is determined by a series of classes $\tilde{c}_i$ in*

$$(11) \qquad H^1\left(\frac{G}{\ker \rho_{i-1}}, k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]\right) \overset{\inf}{\hookrightarrow} H^1(G, k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]) .$$

These cocycles satisfy certain conditions which will be given in eq. (14) and theorem 15. The monomorphism inf is the inflation map in group cohomology, see [28, II.2-3, p. 64].

Remark 12. *The vector space $k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]$ has as base the space of monomials $\bar{f}_0^{\nu_0} \bar{f}_1^{\nu_1} \ldots \bar{f}_{i-1}^{\nu_{i-1}}$, of degree smaller than m, where $\nu_i < p^{n_i}$. The action on them can be described in terms of the binomial theorem, i.e.*
(12)
$$\bar{f}_0^{\nu_0} \bar{f}_1^{\nu_1} \ldots \bar{f}_{i-1}^{\nu_{i-1}} \xrightarrow{\sigma} \bar{f}_0^{\nu_0} \sum_{\mu_1}^{\nu_1} \cdots \sum_{\mu_{i-1}}^{\nu_{i-1}} \binom{\mu_1}{\nu_1} \cdots \binom{\mu_{i-1}}{\nu_{i-1}} \bar{f}_1^{\mu_1} \ldots \bar{f}_{i-1}^{\mu_{i-1}} \bar{c}_1^{\nu_1-\mu_1} \ldots \bar{c}_{i-1}^{\nu_{i-1}-\mu_{i-1}}.$$

2.6. Describing an HKG-cover as a sequence of Artin-Schreier extensions.
It is known, see [7], that every elementary abelian field extension L/K, with Galois group $(\mathbb{Z}/p\mathbb{Z})^n$, is given as an Artin-Schreier extension of the form

$$L = K(y): \qquad y^{p^n} - y = b, \ b \in K.$$

In our case, the elementary abelian field extension F_{i+1}/F_i can be generated by an element $y \in F_{i+1}$ but this element might not be the semigroup generator $\bar{f}_i$. We can give a description of the Artin-Schreier extension F_{i+1}/F_i using an additive monic polynomial

$$A_i(X) = X^{p^{n_i}} + a_{n-1}X^{p^{n_i-1}} + \cdots + a_1 X^p + a_0 X - b_i,$$

which can be computed in terms of the Moore determinant [8]. Let $\{\sigma_1, \ldots, \sigma_{n_i}\}$ be a basis of the Galois group $\mathrm{Gal}(F_{i+1}/F_i) \cong (\mathbb{Z}/p\mathbb{Z})^{n_i}$ and let $w_1, \ldots, w_{n_i}$ be elements of k^* such that $\sigma_j(\bar{f}_i) = \bar{f}_i + w_j$. Let W be the subspace of k spanned by the w_j, $j = 1, \ldots, n_i$. We have $\dim_{\mathbb{F}_p} W = n_i$.

Let $P_i(X) = \prod_{a \in W}(X - a)$. Since every w_i is an element of k, $\mathrm{Gal}(F_{i+1}/F_i)$ acts trivially on $P_i(X)$ and we consider the polynomial

$$A_i(X) := P_i(X) - P_i(\bar{f}_i)$$

Notice that, for a $\sigma \in \mathrm{Gal}(F_{i+1}/F_i)$, we can write $\sigma = \sigma_1^{\nu_1} \circ \cdots \circ \sigma_{n_i}^{\nu_{n_i}}$ and $\sigma(\bar{f}_i + c) = \bar{f}_i + \nu_1 w_1 + \cdots + \nu_{n_i} w_{n_i} + c$ which means that $P_i(\bar{f}_i)$ is $\mathrm{Gal}(F_{i+1}/F_i)$ invariant, i.e. belongs to F_i. Therefore, the polynomial $A_i(X)$ belongs to $F_i[X]$, is monic of degree $p^{n_i} = [F_{i+1} : F_i]$ and vanishes at $\bar{f}_i$ hence it is the irreducible polynomial of $\bar{f}_i$ over F_i. The polynomial $P_i(X)$ is given by

$$P_i(X) = \frac{\Delta(w_1, w_2, \ldots, w_{n_i}, X)}{\Delta(w_1, w_2, \ldots, w_{n_i})},$$

where $\Delta(w_1, \ldots, w_n)$ is the Moore determinant;

$$\Delta(w_1, \ldots, w_n) = \det \begin{bmatrix} w_1 & w_2 & \ldots & w_n \\ w_1^p & w_2^p & \ldots & w_n^p \\ \vdots & \vdots & & \vdots \\ w_1^{p^{n-1}} & w_2^{p^{n-1}} & \ldots & w_n^{p^{n-1}} \end{bmatrix}.$$

It is an additive polynomial of the form

$$P_i(X) = X^{p^{n_i}} + a_{n-1}X^{p^{n_i-1}} + \cdots + a_1 X^p + a_0 X,$$

where $a_i \in k \subset F_i$. We have proved that the generator $\bar{f}_i$ of the extension F_{i+1}/F_i satisfies an equation of the form

(13)
$$\bar{f}_i^{p^{n_i}} + a_{n_i-1}\bar{f}_i^{p^{n_i-1}} + \cdots + a_1 \bar{f}_i^p + a_0 \bar{f}_i = b_i,$$

for some $a_{n_i-1}, \ldots, a_0 \in k$, $b_i = P_i(\bar{f}_i) \in F_i$. We have the following:

Theorem 13. *The cocycles $\bar{c}_i \in H^1(\mathrm{Gal}(F_{i+1}/F_1), k_{\mathbf{n}, \bar{m}_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$, when restricted to the elementary abelian group $\mathrm{Gal}(F_{i+1}/F_i) < \mathrm{Gal}(F_{i+1}/F_1)$ describe fully the elementary abelian extension F_{i+1}/F_i given by the equation*

$$P_i(Y) = b_i.$$

Moreover the element $b_i = P_i(\bar{f}_i)$ is described by the additive polynomial $P_i(Y)$ and by the selection of $\bar{f}_i$. A different selection of $\bar{f}'_i$, i.e. $\bar{f}'_i = \bar{f}_i + a$, for some $a \in k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]$ gives rise to the same polynomial P_i and to a different b'_i given by $b'_i = b_i + P_i(a)$. The two extensions $F_i(\bar{f}_i)$ and $F_i(\bar{f}'_i)$ are equal.

Proof. The only part we didn't prove is the dependence of the additive polynomial to the selection of the generator $\bar{f}_i$. We have seen that changing $\bar{f}_i$ adds a coboundary to $\bar{c}_i$.

But when σ belongs to $\mathrm{Gal}(F_{i+1}/F_i)$, then the $\bar{c}_i(\sigma)$ belongs to k, and k admits the trivial action. Therefore, all coboundaries are zero and the result follows by lemma 11. $\square$

The additive polynomial $P_i(Y)$, which depends on the values of $\bar{c}_i(\sigma)$ with $\sigma \in \mathrm{Gal}(F_{i+1}/F_i)$ gives also compatibility conditions for the cocycle $\bar{c}_i$ on all elements of $\mathrm{Gal}(F_{i+1}/F_1)$. Namely, by application of σ to eq. (13) we obtain the following

(14) $$\boxed{P_i(\bar{c}_i(\sigma)) = (\sigma - 1)b_i \text{ for all } \sigma \in \mathrm{Gal}(F_i/F_1).}$$

So if σ keeps b_i invariant, for instance when $\sigma \in \mathrm{Gal}(F/F_i)$, then $\bar{c}_i(\sigma) \in \mathbb{F}_{p^n} \subset k$.

Equation (14) is essentially a relation among the cocycles $\bar{c}_i(\sigma)$ and $\bar{c}_\nu(\sigma)$ for $\nu < i$. Indeed, the element $b_i \in k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]$ is a polynomial expression on the elements $\bar{f}_0, \ldots, \bar{f}_{i-1}$, and the action is given in terms of the elements $\bar{c}_\nu(\sigma)$ for $\nu < i$ and $\bar{f}_i$ as given in eq. (12).

Lemma 14. *An additive polynomial $P \in k[Y]$ defines a map*

(15) $$H^1(G, k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]) \longrightarrow H^1(G, L(\mu P))$$
$$d \longmapsto P(d),$$

for some $\mu \in \mathbb{N}$ for μ big enough.

Proof. Notice first that elements in the space $L(\nu P)$, for some $\nu \in \mathbb{N}$, can be multiplied as elements of the ring $\mathbf{A}$, so a polynomial expression $P(d)$ of a cocycle d makes sense. One has to be careful since the multiplication of two elements in $L(\nu P)$, is not in general an element of $L(\nu P)$, since it can have a pole order greater than ν. This is the reason why in the right hand side of eq. (15) we have introduced cohomology with values in $L(\mu P)$, for μ big enough. However notice that eq. (14) implies that $P(\bar{c}_i(\sigma)) \in k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]$ so that $P_i(\bar{c}_i) \in H^1(G, k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$.

Finally observe now that if d is a cocycle, i.e. $d(\sigma\tau) = d(\sigma) + \sigma d(\tau)$, then

$$P(d(\sigma\tau)) = P(d(\sigma) + \sigma d(\tau)) = P(d(\sigma)) + P(\sigma d(\tau)) = P(d(\sigma)) + \sigma P(d(\tau)).$$

On the other hand if $d(\sigma) = (\sigma - 1)b$ is a coboundary, then

$$P(d(\sigma)) = P((\sigma - 1)b) = (\sigma - 1)P(b)$$

is a coboundary as well. $\square$

This allows us to give a cohomological interpretation of eq. (14):

Theorem 15. *The cocycles $\bar{c}_i$ given in eq. (11) are in the kernel of the map P_i acting on cohomology as defined in lemma 14. The corresponding element b_i is then the element expressing $P(c_i)$ as a coboundary. The elementary abelian extension is determined by a series of cocycles $\bar{c}_i \in H^1(\mathrm{Gal}(F_{i+1}/F_i), k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$, which define a series of additive polynomials P_i and extend to cocycles in $\bar{c}_i \in H^1(\mathrm{Gal}(F_{i+1}/F_1), k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}])$ so that each $\bar{c}_i$ is in the kernel of P_i.*

3. Nottingham groups

An automorphism σ of the complete local ring $k[[t]]$ is determined by the image $\sigma(t)$ of t, where $\sigma(t) = \sum_{i=1}^{\infty} a_i t^i \in k[[t]]$. We consider the subgroup of normalised automorphisms that is, automorphisms of the form

$$\sigma : t \mapsto t + \sum_{i=2}^{\infty} a_i t^i.$$

Jennings [12] proved that the set of latter automorphisms forms a group under substitution, denoted by $\mathcal{N}(k)$, called the Nottingham group. This group has many interesting properties, for instance Camina proved in [2] that every countably based pro-p group can be embedded, as a closed subgroup, in the Nottingham group. We refer the reader to [3] for more information regarding $\mathcal{N}(k)$. We would like to provide an explicit way to describe the elements of $\mathcal{N}(k)$. It is proved in [16, prop. 1.2] and [18, sec. 4, th. 2.2], that each automorphism of order p is conjugate to the automorphism given by

$$(16) \qquad t \mapsto t(1 + ct^m)^{-1/m} = t \left(\sum_{\nu=0}^{\infty} \binom{-1/m}{\nu} c^{\nu} t^{\nu m} \right)$$

for some $c \in k^{\times}$ and some positive integer m prime to p.

In [1] F. Bleher, T. Chinburg, B. Poonen and P. Symonds, studied the extension $L/k(t)$, where $L := k(\{\sigma(t) : \sigma \in G\})$. Notice here that each automorphism of order p^n is conjugate to $t \mapsto \sigma(t)$, where $\sigma(t) \in k[[t]]$ is algebraic over $k(t)$. Also in [1] the notion of almost rational automorphism is defined: an automorphism $\sigma \in \mathrm{Aut} k[[t]]$ is called almost rational if the extension $L/k(t)$ is Artin-Schreier.

The rational function field $k(t)$, despite its simple form, is not natural with respect to the group G acting on the HKG-cover. For example the determination of the algebraic extension $L/k(t)$ and the group of the normal closure seems very difficult.

Here we plan to give another generalization, by using the fact that the "natural" rational function field with respect to the Katz-Gabber cover is X^{G_1} and not $k(t)$.

In [17, p. 473] the first author proposed the following explicit form for an automorphism of an HKG-cover of order p^n;

$$\sigma(t) = t \left(1 + \sum_{i=1}^{r} c_i(\sigma) u_i t^{m - m_i} \right)^{-1/m},$$

where m is the first pole number which is not divisible by the characteristic p, u_i/t^{m_i} for $1 \le i \le r$ are functions in $L(mP)$ (u_i is a unit) and $1/t^m$ is the function corresponding to m (t being the local uniformizer). In the latter function the unit is absorbed by Hensel's lemma.

3.1. **A canonical selection of uniformizer.** In an attempt to describe in explicit form automorphisms of $k[[t]]$ let us quote here some results from [17]. We will work with the corresponding HKG-cover $X \xrightarrow{G} \mathbb{P}^1$ corresponding to a finite subgroup $G \subset \mathrm{Aut} k[[t]]$. Again let m_r denote the first pole number not divisible by the characteristic and f_i, $i = 1, \ldots, \dim L(m_r P) = r$ a basis for the space $L(m_r P)$, such that

$$(17) \qquad (f_i)_{\infty} = m_i.$$

As we have seen this basis is not unique but eq.(17) implies that if the element f_i is selected, then $f'_i = \lambda_i f_i + a_i$, where $a_i \in L\big((m_i - 1)P\big)$ is also a basis element of valuation m_r.

This means that the base change we will consider, corresponds to invertible upper triangular matrices, i.e. to linear maps which keep the flag of the vector spaces $L(m_iP)$.

Recall that $m = m_r$ is the first pole number not divisible by p. Let us focus on the element f_r. This element is of the form $f_r = u_m/t^m$, where u_m is a unit. Since $(m, p) = 1$ we know by Hensel's lemma that u_m is an m-th power so by a change of uniformizer we can assume that $f_r = 1/t^m$. When changing from a uniformizer t to a uniformizer $t' = \phi(t) = tu(t)$ ($u(t)$ is a unit in $k[[t]]$, then the automorphism $\sigma \in k[[t]]$ expressed as an element in $k[[t']]$ is a conjugate of the initial automorphism, i.e. as $\phi\sigma\phi^{-1}$. By selecting the canonical uniformizer with respect to f_r we see that the expression of an arbitrary σ can take a simpler representation after conjugation. Also this result is in accordance with (and can be seen as a generalization of) the result of Klopsch and Lubin, [16], [18]. The selection of uniformizer $t = t_{f_r}$ is unique once f_r is selected.

Definition 16. *We will call the uniformizer* $t_{f_r} = f_r^{-1/m}$ *the* cannonical uniformizer *corresponding to* f_r.

What happens if we change the function f_r to $f'_r = f_r + a$, where $a \in L((m-1)P)$? Then $a = u/t^\mu$, with $0 \le \mu < m$ and in this case the new uniformizer is given by

$$t_{f'_r} = \left(f_r + \frac{u}{t^\mu}\right)^{-1/m} = t\left(1 + ut^{m-\mu}\right)^{-1/m} = t\left(1 + at^m\right)^{-1/m}.$$

Keep in mind that the set of uniformizers for the local ring $k[[t]]$ equals to $tu(t)$, where u is a unit of the ring $k[[t]]$.

Let $\bar{m}_1, \ldots, \bar{m}_s$ be the generators of the Weierstrass semigroup $H(P)$. These elements correspond to a successive sequence of function fields $F_i = F_{i-1}(\bar{f}_{i-1})$ so that $v(\bar{f}_{i-1}) = p^{|\mathrm{Gal}(F/F_i)|}\lambda_{h-1} = \bar{m}_i$. It is not clear that $\bar{m}_i \ge \bar{m}_j$ for $j < i$. However if for some j we have $\bar{m}_j < \bar{m}_i$ for some $i < j$ then

$$\sigma(\bar{f}_j) = \sigma(\bar{f}_j) + \bar{c}_j(\sigma), \text{ where } \bar{c}_j \in k[\bar{f}_0, \ldots, \widehat{\bar{f}_i}, \ldots, \bar{f}_{j-1}],$$

that is, $\bar{f}_i$ does not appear in any term of the polynomial expression of $\bar{c}_j(\sigma)$, for all $\sigma \in G$. This means that we can generate an HKG-cover with corresponding function field generated by fewer elements than the initial one.

If we assume that among all HKG-covers which correspond to a local action of G on $k[[t]]$ we select one whose function field is minimally generated then $\bar{m}_1 < \bar{m}_2 < \ldots < \bar{m}_s$.

Lemma 17. *Let* $m = m_r$ *be the the first pole number not divisible by the characteristic* p. *Then* $m = \bar{m}_s$, *that is the pole number corresponding to the last generator* $\bar{f}_s$.

Proof. It is clear that not all them are divisible by p since $m \in H(P)$, $p \nmid m$. So at least one generator must be prime to p. On the other hand $F_i = F_{i-1}(\bar{f}_{i-1})$, thus the pole numbers $\bar{m}_i$ of elements $\bar{f}_i$ for $i < s$ are divisible by p, see also [14, eq. (6)]. Therefore only the last generator can be not divisible by p. □

Theorem 18. *Let* $\bar{c}_s \in H^1(G, k_{\mathbf{n}, m_{i+1}}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{s-1}])$ *be the cocycle corresponding to* $m = m_s$, *where* m *is the first pole number not divisible by* p, *see lemma 17. We choose as uniformizer the canonical uniformizer* $t = \bar{f}_s^{-1/m}$. *Then we can define the representation:*

$$\Phi : G \longrightarrow \mathrm{Aut}(k[[t]])$$

(18)
$$\sigma \longmapsto t \mapsto t(1 + \bar{c}_s(\sigma)t^m)^{-1/m},$$

where the last expression gives rise to a powerseries by expanding it using the binomial theorem (also recall that an automorphism of $k[[t]]$ *is known its action on* t *is*

known). We have that for all $\sigma, \tau \in G$

$$\Phi(\tau\sigma) = \Phi(\sigma)\Phi(\tau).$$

Furthermore Φ is a monomorphism.

Proof. We begin by noticing that $\sigma(\bar{f}_s) = \bar{f}_s + \bar{c}_s(\sigma)$ and if we select t so that $t^{-m} = \bar{f}_s$, then we can solved in terms of $\sigma(t)$ to give the image of $\Phi(\sigma) \in \mathrm{Aut}(k[[t]])$ in eq. (18).

Recall that $\sigma \in G$ acts on the elements $\bar{f}_0, \ldots, \bar{f}_{s-1}$ by definition in terms of the cocycles $\bar{c}_i(\sigma)$. This was defined to be a left action. Also this action is by construction assumed to be compatible with the action of G on $k[[t]]$ in the sense that when we see the elements $\bar{f}_i$ as elements in $k[[t]][t^{-1}]$, then $\sigma(\bar{f}_i) = \Phi(\sigma)(\bar{f}_i)$, that is the action of σ on $\bar{f}_i$ as elements in $k_{\mathbf{n}, m_{i+1}}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{s-1}]$ coincides with the action of σ on f_i seen as an element in the quotient field of $k[[t]]$. In other words we have

$$\sigma(f_i(t)) = f_i(\sigma(t)) = f_i(t) + c_i(\sigma).$$

We will prove first that this is a homomorphism i.e.

$$(19) \qquad t(1 + \bar{c}_s(\tau\sigma)t^m))^{-1/m} = t(1 + \bar{c}_s(\sigma)t^m)^{-1/m} \circ t(1 + \bar{c}_s(\tau)t^m)^{-1/m},$$

where $\circ$ denotes the composition of two powerseries. The right hand side of the above equation equals

$$t\left(1 + \bar{c}_s(\tau)t^m\right)^{\frac{-1}{m}}\left(1 + \frac{\tau(\bar{c}_s(\sigma))t^m}{1 + \bar{c}_s(\tau)t^m}\right)^{\frac{-1}{m}} = t\left(1 + \left(\bar{c}_s(\tau) + \tau\bar{c}_s(\sigma)\right)t^m\right)^{-1/m}$$

so eq. (19) holds by the cocycle condition for $\bar{c}_s$.

The kernel of the homomorphism Φ, consists of all elements $\sigma \in G$ such that $\bar{c}_s(\sigma) = 0$. But if $\bar{c}_s(\sigma) = 0$ then $\sigma(t) = t$ and σ is the identity. $\square$

Remark 19. *The above construction behaves well when we change f_m to $f'_m = f_m + a$. In any case the representation given in eq. (18) is given in terms of the canonical uniformizer t_{f_r} corresponding to the element $\bar{f}_s = f_r$ which gives rise to the cocycle $\bar{c}_s$.*

Remark 20. *Equation (18) implies that the knowledge of the cocycle $\bar{c}_s$ implies the knowledge of $\sigma(t)$, which in turn gives us how σ acts on all other elements $\bar{f}_i$ for all $0 \leq i \leq s-1$. This seems to imply that $\bar{c}_s$ can determine all other cocycles $\bar{c}_\nu$ for all $1 \leq \nu \leq s-1$. This is not entirely correct. Indeed, $\bar{c}_s$ is a cocycle with values on the G-module $k_{\mathbf{n}, m_s}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{s-1}]$, therefore the action of G on $\bar{f}_i$ for $0 \leq i \leq s-1$ is assumed to be known and is part of the definition of the cocycle $\bar{c}_s$. This means that $\bar{c}_i$ are assumed to be known and part of the definition of $\bar{c}_s$.*

Proposition 21. *If $\sigma \in G$ then*

$$v_P(\sigma(t) - t) = m - v_P(\bar{c}_s(\sigma)) + 1 = I(\sigma),$$

where $I(\sigma)$ is the Artin character since k is algebraically closed, see [23, VI.2]. Therefore $\sigma \in G_{I(\sigma)} - G_{I(\sigma)+1}$.

Proof. The valuation of $\sigma(t) - t$ comes from the binomial expansion of eq. (18). The rest is the definition of the ramification group. $\square$

3.2. **Application: Elements of order p^h in the Nottingham group.**

3.2.1. *On the form of elements of order p.* It is known that every element of order p in $\mathrm{Aut}(k[[t]])$ is conjugate to the automorphism

$$t \mapsto t(1 + ct^m)^{-1/m}, \quad \text{where } c \in k,$$

for some m prime to p, see [16, prop. 1.2] and [18, th. 2.2].

We can obtain this result using theorem 18. Let σ be an automorphism of $k[[t]]$ of order p. Let $X \to \mathbb{P}^1$ be the corresponding HKG-cover. The sequence of higher ramification groups equals $\langle \sigma \rangle = G_0 = G_1 = \cdots = G_m > \{1\}$, i.e. there is only one jump in the ramification filtration. If $m = 1$ then $G_i(P) = \{1\}$ for $i \geq 2$ and in this case the genus $g_X = 0$. This is a trivial case so we can assume that $m > 1$. From theorem 5 we know that the Weierstrass semigroup is minimaly generated by $p = |G_1(P)|$ and m_r. If m_i is a pole number less than m_r then m_i is a multiple of p, hence the corresponding elements f_i with pole order m_i at P will be powers of f_0 where $(f_0)_\infty = pP$.

Since the ramification filtration jumps only once, the same holds for the representation filtration, i.e.

$$G_1(P) = \mathrm{Ker}\rho_{c_1} > \{1\}$$

So if σ is not the identity then by [14, prop.27] we have that

$$\sigma(f_0^i) = f_0^i \text{ for } i = 0, 1, \ldots, \lfloor m_r/p \rfloor \text{ and}$$

$$\sigma(f_{c_1+1}) = \sigma(f_r) = f_r + c(\sigma) \text{ where } c(\sigma) \in k^\times.$$

Compare also with the computation of proposition 21. To obtain the result we notice the following; changing the local uniformizer to canonical one imposes the substitution of σ by a conjugate which, by theorem 18, maps t to desired form.

3.2.2. *Application to the case of cyclic groups.* Let us now consider an element σ of order p^h. As before the cyclic group

$$G_0(P) = G_1(P) = \cdots = G_{b_1}(P) \gneqq G_{b_1+1}(P) = \cdots = G_{b_2}(P) \gneqq \cdots \gneqq G_{b_\mu}(P) \gneqq \{1\}$$

Since a cyclic group has only cyclic subgroups and all quotients of cyclic groups are cyclic, while $G_{b_i}/G_{b_{i+1}}$ is elementary abelian, we see that the number of gaps μ is equal to h. and p^{h-i} is the exact power of p dividing each $\bar{m}_i$.

Observe that all intermediate elementary abelian extensions $F_{i+1}/F_i = F_i(\bar{f}_i)/F_i$ are cyclic. The additive polynomial describing the extension $F_i(\bar{f}_i)/F_i$ is given by

$$Y^p - \bar{c}_i^{p-1}Y = \bar{f}_i^p - \bar{c}_i^{p-1}\bar{f}_i,$$

by computation of the Moore determinant $\det \begin{pmatrix} c_i & Y \\ c_i^p & Y^p \end{pmatrix}$, where $\bar{c}_i$ is computed at a generator σ^{p^i} of the cyclic group $\mathrm{Gal}(F_{i+1}/F_i) = G_{b_{i+1}}/G_{b_i}$, (i.e. $\sigma^{p^i}(\bar{f}_i) = \bar{f}_i + \bar{c}_i(\sigma^{p^i})$). Since $\bar{c}_i \in k$, if we rescale $\bar{f}_i$ by $\bar{f}_i/c_i$, we can assume without loss of generality that the equation is an Artin-Schreier one:

$$Y^p - Y = \bar{f}_i^p - \bar{f}_i = b_i, \text{ where } b_i \in F_i.$$

Let g be an automorphism of the HKG-cover X. Since $g(\bar{f}_\nu) = \bar{f}_\nu + \bar{c}_\nu(g)$ and $\bar{c}_\nu(g) \in F_{\nu-1}$, the automorphism g gives rise to an automorphism $g : F_\nu \to F_\nu$ for all ν. We have that
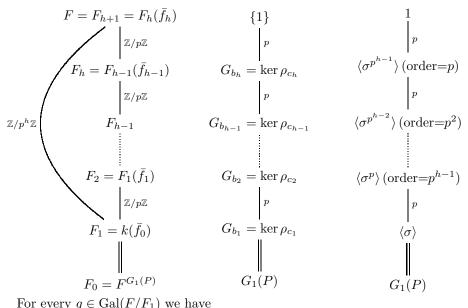
(20) $$\bar{c}_i(g)^p - \bar{c}_i(g) = (g-1)(\bar{f}_i^p - \bar{f}_i) = (g-1)b_i.$$

Notice that eq. (20) has many solutions $\bar{c}_i(g)$ for a fixed g, which differ by an element $\bar{c}_i(\sigma)$ for some $\sigma \in \mathrm{Gal}(F_{i+1}/F_i)$, since $(g\sigma - 1)(b_i) = (g-1)(b_i)$.

The representation filtration has the following form (the filtrations are collectively depicted in the diagrams below)

$$F^{G_1(P)} = F_0 = F^{\mathrm{ker}\rho_0} \subset F_1 = F^{\mathrm{ker}\rho_1} \subset \cdots \subset F_r = F^{\mathrm{ker}_r} = F.$$

We have $p^{h-i} = |\ker \rho_{c_{i+1}}|$ for $0 \le i \le n-1$ and $p^h = |G_1(P)|$. The generators of the Weierstrass semigroup are $p^h, p^{h-1}\lambda_1, \ldots, p\lambda_{\mu-1}, \lambda_\mu$. We have the following tower of fields:

$$
\begin{array}{ccc}
F = F_{h+1} = F_h(\bar{f}_h) & \{1\} & 1 \\
\Big|\, \mathbb{Z}/p\mathbb{Z} & \Big|\, p & \Big|\, p \\
F_h = F_{h-1}(\bar{f}_{h-1}) & G_{b_h} = \ker \rho_{c_h} & \langle \sigma^{p^{h-1}} \rangle \,(\text{order}=p) \\
\Big|\, \mathbb{Z}/p\mathbb{Z} & \Big|\, p & \Big|\, p \\
F_{h-1} & G_{b_{h-1}} = \ker \rho_{c_{h-1}} & \langle \sigma^{p^{h-2}} \rangle \,(\text{order}=p^2) \\
\vdots & \vdots & \vdots \\
F_2 = F_1(\bar{f}_1) & G_{b_2} = \ker \rho_{c_2} & \langle \sigma^p \rangle \,(\text{order}=p^{h-1}) \\
\Big|\, \mathbb{Z}/p\mathbb{Z} & \Big|\, p & \Big|\, p \\
F_1 = k(\bar{f}_0) & G_{b_1} = \ker \rho_{c_1} & \langle \sigma \rangle \\
\Big\| & \Big\| & \Big\| \\
F_0 = F^{G_1(P)} & G_1(P) & G_1(P)
\end{array}
$$

(with $\mathbb{Z}/p^h\mathbb{Z}$ spanning the left tower)

For every $g \in \mathrm{Gal}(F/F_1)$ we have

$$ g(\bar{f}_{r-1}) - \bar{f}_{r-1} = \bar{c}_{r-1}(g). $$

For a cyclic group $\mathbb{Z}/p^i\mathbb{Z}$ the cohomology is given by:

$$ H^1(\mathbb{Z}/p^i\mathbb{Z}, A) = \frac{\{a \in A : N(a) = 0\}}{(\sigma_i - 1)A}, $$

where σ_i is a generator of the cyclic group $\mathbb{Z}/p^i\mathbb{Z}$ and $N = 1 + \sigma + \cdots + \sigma^{p^i-1}$ is the norm, see [27, th. 6.2.2, p. 168]. In view of theorem 15 we will consider the groups $\mathrm{Gal}(F_{i+1}/F_1)$, which are generated by the generator σ of the cyclic group $\mathrm{Gal}(F_{h+1}/F_1)$ modulo the subgroup $\mathrm{Gal}(F_{h+1}/F_{i+1})$. Thus in the group $\mathrm{Gal}(F_{i+1}/F_1)$ the order of σ equals p^i.

Observe now that $\tau = \sigma^{p^{i-1}}$ acts trivially on $A = k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]$. We now compute the norm for $\mathrm{Gal}(F_{i+1}/F_1)$:

$$
1 + \sigma + \cdots + \sigma^{p^i-1} = \sum_{\nu=0}^{p^i-1} \sigma^\nu = \sum_{\pi=0}^{p-1} \sum_{\upsilon=0}^{p^{i-1}-1} \sigma^{\pi p^{i-1}} \sigma^\upsilon
$$
$$
= \sum_{\pi=0}^{p-1} \tau^\pi \sum_{\upsilon=0}^{p^{i-1}-1} \sigma^\upsilon
$$

where $\tau := \sigma^{p^{i-1}}$, and observe that the above equation restricted on A gives

$$
1 + \sigma + \cdots + \sigma^{p^i-1} = p \cdot \sum_{\upsilon=0}^{p^{i-1}-1} \sigma^\upsilon
$$

which is zero on A. So we finally arrive at the computation:

$$
H^1\left(\mathbb{Z}/p^i\mathbb{Z}, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]\right) = k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \ldots, \bar{f}_{i-1}]_{\mathbb{Z}/p^i\mathbb{Z}},
$$

where the later space is the space of $\mathbb{Z}/p^i\mathbb{Z}$-coinvariants.

Proposition 22. *A cyclic group of the Nottingham group is described by a series of elements* $\bar{c}_i \in k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \ldots, \bar{f}_{i-1}]_{\mathbb{Z}/p^i\mathbb{Z}}$ *so that* $\bar{c}_i^p - \bar{c}_i$ *is zero in the space* $k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \ldots, \bar{f}_{i-1}]_{\mathbb{Z}/p^i\mathbb{Z}}$.

In order to ensure that the element σ has order p^h we should have, $\bar{c}_s(\sigma^{p^\nu}) \neq 0$, for all $0 \leq \nu < h$ i.e.

$$\left(1 + \sigma + \cdots + \sigma^{p^\nu - 1}\right)\bar{c}(\sigma) \neq 0.$$

References

[1] Frauke M. Bleher, Ted Chinburg, Bjorn Poonen, and Peter Symonds. Automorphisms of Harbater–Katz–Gabber curves. *Mathematische Annalen*, 368(1):811–836, Jun 2017.

[2] Rachel Camina. Subgroups of the Nottingham group. *Journal of Algebra*, 196(1):101–113, 1997.

[3] Rachel Camina. The Nottingham group. In *New horizons in pro-p groups*, pages 205–221. Springer, 2000.

[4] T. Chinburg, R. Guralnick, and D. Harbater. Oort groups and lifting problems. *Compos. Math.*, 144(4):849–866, 2008.

[5] Ted Chinburg, Robert Guralnick, and David Harbater. The local lifting problem for actions of finite groups on curves. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(4):537–605, 2011.

[6] Ted Chinburg, Robert Guralnick, and David Harbater. Global Oort groups. *J. Algebra*, 473:374–396, 2017.

[7] Arnaldo Garcia and Henning Stichtenoth. Elementary abelianp-extensions of algebraic function fields. *manuscripta mathematica*, 72(1):67–79, Dec 1991.

[8] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[9] David Harbater. Moduli of p-covers of curves. *Communications in Algebra*, 8(12):1095–1122, 1980.

[10] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[11] Nathan Jacobson. *Basic algebra. II*. W. H. Freeman and Company, New York, second edition, 1989.

[12] Stephen Arthur Jennings. Substitution groups of formal power series. *Canad. J. Math*, 6:325–340, 1954.

[13] Sotiris Karanikolopoulos. On holomorphic polydifferentials in positive characteristic. *Mathematische Nachrichten*, 285(7):852–877, Jan 2012.

[14] Sotiris Karanikolopoulos and Aristides Kontogeorgis. Automorphisms of curves and Weierstrass semigroups for Harbater-Katz-Gabber covers. *Transactions of the American Math. Soc. (accepted), arXiv preprint arXiv:1302.2528*, 2013.

[15] Nicholas M Katz. Local-to-global extensions of representations of fundamental groups. *Ann. Inst. Fourier (Grenoble)*, 36(4):69–106, 1986.

[16] Benjamin Klopsch. Automorphisms of the Nottingham group. *Journal of Algebra*, 223(1):37–56, 2000.

[17] Aristides Kontogeorgis. The ramification sequence for a fixed point of an automorphism of a curve and the weierstrass gap sequence. *Mathematische Zeitschrift*, 259(3):471–479, 2008.

[18] Jonathan Lubin. Torsion in the Nottingham group. *Bulletin of the London Mathematical Society*, 43(3):547–560, 2011.

[19] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[20] Andrew Obus. The (local) lifting problem for curves. In *Galois-Teichmüller theory and arithmetic geometry*, volume 63 of *Adv. Stud. Pure Math.*, pages 359–412. Math. Soc. Japan, Tokyo, 2012.

[21] Andrew Obus and Stefan Wewers. Cyclic extensions and the local lifting problem. *Ann. of Math. (2)*, 180(1):233–284, 2014.

[22] Florian Pop. The Oort conjecture on lifting covers of curves. *Ann. of Math. (2)*, 180(1):285–322, 2014.

[23] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.

[24] I. R. Shafarevich. Abelian and nonabelian mathematics. *Math. Intelligencer*, 13(1):67–75, 1991. Translated from the Russian by Smilka Zdravkovska.

[25] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[26] Djurre Tijsma. Automata and finite order elements in the Nottingham group. Master's thesis, Utrecht University, 2018.

[27] Charles A. Weibel. *An introduction to homological algebra*. Cambridge University Press, Cambridge, 1994.

[28] Edwin Weiss. *Cohomology of groups*. Academic Press, New York, 1969.

Department of Mathematics, National and Kapodistrian University of Athens, Panepistimioupolis, 15784 Athens, Greece

E-mail address: `kontogar@math.uoa.gr`

URL: `http://users.uoa.gr/~kontogar`

Department of Mathematics, National and Kapodistrian University of Athens, Panepistimioupolis, 15784 Athens, Greece

E-mail address: `iotsouknidas@math.uoa.gr`